Data Sheet

McAfee Foundstone Professional Services Data Risk Assessment

We help you meet your compliance requirements.

Most organizations that process, store, or transmit customer data (PCI, PII, PHI, etc.) are subject to regulatory oversight. Organizations including, but not limited to credit card brands, HHS, and the FFIEC require organizations to build and maintain their information security programs based on annual risk assessments. These assessments are very useful to understand the security posture of your organization. They lead to an inventory and classification of data systems, identification of threats and vulnerabilities, and the determination of high-risk issues, so that your organization can better protect your customer data.

Risk Assessment Process

Phase 1—Impact Analysis/ Data Identification

- Identify the data owners.
- Identify the data systems and customer data environment.
  - Identify the customer data environment.
  - Identify the data owners.
  - Discover customer data flows.
- Validate data classification.
- Determine business impact of a data breach.
  - Reputation.
  - Customer defection.
  - Financial loss.

McAfee® Foundstone® Professional Services—part of the Intel® Security product and services offering—delivers a cost-effective process that meets all requirements for periodic risk assessments for PCI, HIPAA, GLBA, and FISMA requirements, among others.

Our Risk Assessment methodology adheres to NIST SP 800-30, and is based on industry accepted Data Security Controls[1] designed to reduce vulnerabilities to threats. The process is delivered as a single engagement with four phases described in this data sheet. The McAfee Foundstone Data Risk Assessment service is scalable to meet a variety of customer budgets and needs for assessing the current state of any data security program. To bring the service full circle, guidance is provided on risk treatment and strategy for building a roadmap to remediate findings.

Scope

The scope of the engagement is custom fit to your organization's needs. The base risk assessment is conducted through interviews and the review of policies, procedures, and reports. This includes tactical security testing such as web application and database security assessments, vulnerability scans, and penetration tests performed by your organization or third-parties. The scope can be expanded by including Data Loss Analysis[2] using the McAfee Data Loss Prevention solution, verification of regulatory scope, and security testing performed by McAfee Foundstone Professional Services.

The in-scope environment primarily includes the Customer Data Environment[3] (CDE) based on the data defined by your organization. From a technology perspective, the CDE is the network(s) that host systems that process, store, or transmit customer data. However, this environment is also comprised of people and processes that handle customer data.

Risk Assessment Process (continued)

Phase 2—Threat Analysis

- Identify threat sources (agents) and events.
  - Accidental and adversarial.
  - Internal and external cyber threats.
  - Physical threats (theft and destruction).
- Evaluate capabilities and motivation of agents.
- Determine the prevalence of agents and events.

Phase 3—Vulnerability Analysis

- Evaluate the sufficiency of policies, procedures, security operations, and other countermeasures in place to control risks.
- Identify vulnerabilities and predisposing conditions.
- Determine the likelihood of a threat event succeeding.

Phase 4—Determine Risk

- Determine the likelihood of a threat event adversely impacting customer data and the business.

Approach

We use asset/impact-oriented analysis that begins with the identification of high-value assets and the identification of impact based on data classification. This is followed by threat and vulnerability analysis and the process concludes with the determination of risk.

Your organization's data risk management processes are evaluated based on their effectiveness and integration into four key areas: 1) security governance, 2) data risk management, 3) data operations, and 4) the information security program.

Deliverables

The risk assessment report includes a separate executive summary as well as the following:

- Summary of findings and recommendations.
- Impact analysis.
- Strategy for remediation roadmap.
- Detailed risk analysis.
- Threat analysis.
- Risk treatment guidelines.
- Vulnerability analysis.

The McAfee Foundstone Difference

Our Data Risk Assessment provides you with the fundamental elements necessary to support or implement an effective risk-based data management program.

All McAfee Foundstone projects are managed using our proven Security Engagement Process (SEP) for project management. A pivotal aspect of this process is continual communication with your organization to ensure the success of your consulting engagements.

Learn More about McAfee Foundstone Professional Services

Fill the gaps in your information security program with trusted advice from McAfee Foundstone Professional Services—part of the Intel Security global professional services organization that provides security consulting, customized product deployments, and training and advisory services. Let our consultants help your organization assess current policies, create new programs that meet compliance goals, and cost-effectively prepare for security emergencies. Speak with your technology advisor about integrating our services or email us at **consulting@foundstone.com**. You can get more information at **www.foundstone.com**.

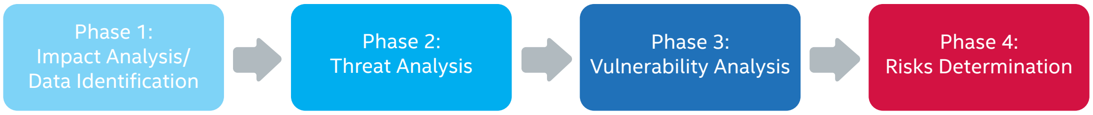

Figure 1. The McAfee Foundstone phased approach to Engagement Lifecycle Management.

[1] A consolidated collection of NIST and PCI controls.

[2] DLA determines if data is successfully contained within the customer data environment, and detects data leakage.

[3] Networks that host systems that process, store, or transmit customer data.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com